LOFTUS & EISENBERG, LTD.
ROSS M. GOOD, ESQ.
(*admitted pro hac vice*)
161 N. Clark, Suite 1600
Chicago, Illinois 60601
T: (312) 772-5396
ross@loftusandeisenberg.com

ARON LAW FIRM
WILLIAM ARON, ESQ. (#234408)
15 W Carrillo St, Suite 217
Santa Barbara, CA 93101
T: (805) 618-1768
bill@aronlawfirm.com
Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT—NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

MELANIE BERMAN, JULIA HAWKINS, LISA JONES, LYON LEIFER, AND KATHLEEN CANFIELD LOFTUS, Plaintiffs, v. 23ANDME, INC. Defendant.	Case No.: 23-CV-00287 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiffs, Melanie Berman ("Berman"), Lisa Jones ("Jones"), Lyon Leifer ("Leifer"), Kathleen Canfield Loftus ("Loftus"), Julia Hawkins ("Hawkins") (collectively "Plaintiffs"), bring this Class Action Complaint against 23andMe ("23andMe" or "Defendant") in their respective individual capacities and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. 23andMe is a genomics and biotechnology company based in South San Francisco, California that provides a direct-to-consumer genetic testing service in which customers provide a saliva sample that is laboratory analyzed, using single nucleotide polymorphism genotyping, to generate reports relating to the customer's ancestry and genetic predispositions to health-related topics.

2. On or about October 6, 2023, 23andMe announced on its website that customer profile information was compiled from individual 23andMe.com accounts without account users' authorization that contained both the personally identifiable information ("PII") and protected health information ("PHI") of its customers (collectively, "Private Information").[1] The exposed Private Information may include names, sex, date of birth, genetic information[2], genetic ancestry results, profile photos and geographical information. (the "Data Breach"). However, Defendant has not disclosed when this Data Breach occurred and for how long.

[1] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d et seq. ("HIPAA"), protected health information ("PHI") is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. Summary of the HIPAA Privacy Rule, available at: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Oct. 12, 2023).

[2] Genetic information is health information protected by the Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/faq/354/does-hipaa-protect-genetic-information/index.html

3. To date, Defendant has not yet disclosed full details of the Data Breach including when it occurred and the length of the exposure of Plaintiffs' and Class Members' PII or the results and findings of any investigation it undertook. Without such disclosure, questions remain as to the full extent of the cyberattack, the number of customers involved, the actual data compromised, and what measures, if any, Defendant has taken to secure the Private Information still in its possession.

4. Defendant has failed to provide direct notice to Plaintiffs and Class Members and so they are unclear about many of the details surrounding the Data Breach, requiring Plaintiffs to spend time and money taking additional steps to protect themselves from the harmful effects of the Data Breach.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect customers' Private Information. Upon information and belief, the mechanism of the cyberattack and the potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to 23andMe, and thus 23andMe was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

6. Defendant disregarded the rights of Plaintiffs and Class Members by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have reasonable or adequately robust computer systems and security practices to safeguard customers' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice regarding the Data Breach.

7. As a result of Defendant's failure to implement and follow reasonable security procedures, Plaintiffs' and Class Members' Private Information is now in the hands of, and has been viewed by, identity thieves. Plaintiffs and Class Members have suffered identity theft and

fraud, have had to spend—and will continue to spend—significant amounts of time and/or money in an effort to protect themselves from the adverse ramifications of the Data Breach, and will forever be at a heightened risk of identity theft and fraud.

8. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiffs' and Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

9. Plaintiffs, on behalf of all others similarly situated, allege claims for (1) negligence; (2) invasion of privacy; (3) breach of contract; (4) breach of implied contract; (5) unjust enrichment; (6) violation of the California Unfair Competition Law (Cal. Business & Professions Code § 17200, et seq.) for unlawful, fraudulent, and unfair business practice; (7) violation of the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq*.); (8) violation of California Consumers Privacy Act (Cal. Civ. Code § 17598.82 *et seq*. and (9) injunctive and declaratory relief.

10. The Illinois Sub-Class alleges violation of Illinois Genetic Information Privacy Act, 410 ILCS 513/1, *et seq*. and Illinois Consumer Fraud Act, 815 ILCS § 505, *et seq*.

11. The Wisconsin Sub-Class alleges violation of Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§100.18, *et seq*. and Breach of Confidentiality of Health Records, Wis. Stat. 146.81, *et seq*.

12. Plaintiffs seek remedies including, but not limited to, compensatory damages for identity theft, fraud, and time spent, reimbursement of out-of-pocket costs, adequate credit monitoring services funded by Defendant, and injunctive relief including improvements to Defendant's data security systems and practices to ensure they have reasonably sufficient security practices to safeguard customers' Private Information that remains in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future.

13. As a direct and proximate result of Defendant's wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, Plaintiffs have incurred (and will continue to incur) economic damages, and other actual injury and harm, in the form of (i) actual identity theft or identity fraud; (ii) the untimely and/or inadequate notification of the Data Breach; (iii) unauthorized disclosure of their PII; (iv) breach of the statutorily-protected confidentiality of their PII; (v) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud caused by the Data Breach; (vi) the value of their time spent mitigating the impact of the Data Breach and mitigating increased risk of identity theft and/or identity fraud; (vii) deprivation of the value of their PII, for which there is a well-established national and international market; and (vii) the impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

PARTIES

14. Plaintiff Melanie Berman is domiciled in Illinois and a customer of 23andMe.

15. Plaintiff Julia Hawkins is domiciled in Iowa and a customer of 23andMe.

16. Plaintiff Lisa Jones is domiciled in Illinois and a customer of 23andMe.

17. Plaintiff Lyon Leifer is domiciled in Illinois and a customer of 23andMe.

18. Plaintiff Kathleen Canfield Loftus is domiciled in Wisconsin and a customer of 23andMe.

19. Defendant 23andMe, Inc. is a Delaware corporation, with its principal place of business at 223 N Mathilda Ave., Sunnydale, CA 94086. It can be served through its registered agent: Corporation Service Company d/b/a CSC – Lawyers Incorporating Service at 2710 Gateway Oaks Dr., Sacramento, CA 95833.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one

member of the class is a citizen of a state different from Defendant. The Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

21. This Court has personal jurisdiction over Defendant because 23andMe is headquartered in California, its principal place of business is in California, and it regularly conducts business in California.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District, and 23andMe is in this District, and has caused harm to Plaintiffs and Class Members residing in this District.

STATEMENT OF FACTS

A. 23andMe's Business Model

23. 23andMe was founded in 2006 and began offering direct-to-consumer genetic testing in November 2007 in which customers provide a saliva sample that is laboratory analyzed, using single nucleotide polymorphism genotyping, to generate reports relating to the customer's ancestry and genetic predispositions to health-related topics and results are posted online.

24. 23andMe provides DNA test kits that are a direct-to-consumer form of genetic testing. These genetic testing kits yield information about your health, genetic traits, and ancestry. After a customer provides their saliva sample, they register the collection tube using the barcode and then mail it back. 23andMe offers a health and ancestry service which includes health reports on genetic health risk, carrier status, wellness, and pharmacogenetics. 23andMe also offers an annual membership that contains everything in the health and ancestry service plus access to ongoing genetic insights. Each of these services and membership have different costs.

25. Due to the nature of these services, 23andMe must store customers' Private Information in its system. 23andMe accomplishes this by keeping the Private Information electronically. 23andMe has more than 14 million customers worldwide and as of December 2022 has genotyped over 5,000,000 individuals.

26. Customers demand security to safeguard their Private Information. 23andMe is required to ensure that such private, personal information is not disclosed or disseminated to

unauthorized third parties without the customers' express, written consent, as further detailed below.[3]

B. The Data Breach

27. On October 6, 2023, Defendant announced in a Blog on its website that customers' accounts had been accessed by unauthorized individuals. The announcement titled "Addressing Data Security Concerns" stated the following:

> We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users' authorization.
>
> After learning of suspicious activity, we immediately began an investigation. While we are continuing to investigate this matter, we believe threat actors were able to access certain accounts in instances where users recycled login credentials - that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked.
>
> We believe that the threat actor may have then, in violation of our Terms of Service, accessed 23andMe.com accounts without authorization and obtained information from certain accounts, including information about users' DNA Relatives profiles, to the extent a user opted into that service.[4]

28. In addition, the Defendant touted its commitment to safety and security in its announcement stating the following:

> 23andMe is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected. We are continuing to investigate to confirm these preliminary results. We do not have any indication at this time that there has been a data security incident within our systems, or that 23andMe was the source of the account credentials used in these attacks.
>
> At 23andMe, we take security seriously. We exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected. When we receive information through those processes or from other sources claiming customer data has been accessed by unauthorized individuals, we immediately investigate to validate whether this information is accurate. Since 2019 we've offered and encouraged

[3] www.23andme.com
[4] https://blog.23andme.com/articles/addressing-data-security-concerns

> users to use multi-factor authentication (MFA), which provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords.[5]

29. However, Defendant failed to send individual notices to affected customers and their Blog notification fails to disclose how many individuals were affected, what information was accessed other than "customer profile information" and "information about users' DNA Relatives profiles" ,and when and for how long the information was accessed.

30. 23andMe's Notice of Data Breach was woefully deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed its employee's e-mail account, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach was a system-wide breach, whether servers storing information were accessed, and how many customers were affected by the Data Breach. Even worse, 23andMe has not offered any identity monitoring to Plaintiffs and other Class Members.

31. Plaintiffs' and Class Members' Private Information is already for sale to criminals on the dark web meaning unauthorized parties have accessed and viewed Plaintiffs' and Class Members' unencrypted, unredacted information.

32. In fact, on October 7, 2023, NBC News reported and confirmed the following:

> A database that has been shared on dark web forums and viewed by NBC News has a list of 999,999 people who allegedly have used the service. It includes their first and last name, sex, and 23andMe's evaluation of where their ancestors came from. The database is titled "ashkenazi DNA Data of Celebrities," though most of the people on it aren't famous, and it appears to have been sorted to only include people with Ashkenazi heritage.[6]

33. In addition, NBC News further reported that "A user on a popular hacker forum had claimed to have made a larger database of users for sale earlier this week."[7]

---

[5] *Id.*

[6] https://www.nbcnews.com/news/us-news/23andme-user-data-targeting-ashkenazi-jews-%20leaked-online-rcna119324

[7] *Id.*

34. This Private Information disclosure which includes almost one million people of Ashkenazi heritage is even more concerning and frightening given the almost simultaneous attack on Israel.

35. On October 9, 2023, 23andMe updated its October 6, 2023, announcement and failed to disclose any useful additional information other that their investigation continues, they "engaged the assistance of third-party forensic experts and are working with "federal law enforcement officials."[8]

C. Plaintiffs ' Efforts to Secure Their Private Information.

36. In order to use Defendant's services, Plaintiffs were required to provide PII to Defendant and expected that their information would be kept confidential.

37. Plaintiffs suffered actual injury from having her Private Information exposed as a result of the Data Breach including, but not limited to (a) paying monies to Defendant for its goods and services which he would not have had Defendant disclosed that it lacked data security practices adequate to safeguard patients' Private Information from theft; (b) damages to and diminution in the value of her Private Information-a form of intangible property that Plaintiffs entrusted to 23andMe as a condition for their services; (c) loss of her privacy; (d) lost time; and (e) imminent and impending injury arising from the increased risk of fraud and identity theft.

38. As a result of the Data Breach, Plaintiffs will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

D. 23andMe's Privacy Policies.

39. 23andMe makes numerous promises to its customers that it will maintain the security and privacy of their Private Information. On its website under Privacy, 23andMe states that:

> "Your privacy comes first. When you explore your DNA with 23andMe, you entrust us with important personal information. That's why, since day one, protecting your privacy has been our number one priority. We're committed to providing you with a safe place where you can learn about your DNA knowing your privacy is protected."

[8] https://blog.23andme.com/articles/addressing-data-security-concerns

> We exceed industry data protection standards and have achieved 3 different ISO certifications to demonstrate the strength of our security program.
>
> We encrypt all sensitive information and conduct regular assessments to identity security vulnerabilities and threats. [9]

40. 23andMe further touts on its website under Privacy[10] the following states:

> Your data is fiercely protected by security practices that are regularly reviewed and updated.
>
> Your genetic information deserves the highest level of security, because without security, you can't have privacy. 23andMe employs software, hardware, and physical security measures to protect your data. And while no security standard or system is bulletproof, we're doing everything in our power to keep your personal data safe.

41. On its website in response to the question "What do you do to stay a step ahead of hackers?" 23andMe states "We take multiple steps. First of all, third-party security experts regularly conduct audits and assessments of our systems, ensuring we will never let our guard down. We encrypt all sensitive information, both when it is stored and when it is being transmitted, so that we make it difficult for potential hackers to gain access."[11]

42. In its Privacy Statement, under Security Measures, 23andMe states that "We implement physical, technical, and administrative measures aimed at preventing unauthorized access to or disclosure of your Personal Information. Our team regularly reviews and improves our security practices to help ensure the integrity of our systems and your Personal Information."[12]

43. 23andMe further states in its Privacy Statement the following:

> We believe everyone deserves a safe place to discover and understand their DNA, which means we need to keep our platform a safe place for all. We use information to monitor, detect, prevent, investigate and mitigate any suspected or actual fraud, prohibited or illegal behaviors on our Services, to combat spam, and other behaviors or actions that break the promises we outline in our Terms of Service.[13]

---

[9] https://www.23andme.com/privacy/
[10] *Id.*
[11] *Id.*
[12] https://www.23andme.com/legal/privacy/full-version/
[13] https://www.23andme.com/legal/how-we-use-info/

44. 23andMe describes how it may use and disclose Private Information for each category of uses or disclosures, none of which provide it a right to expose customers' Private Information in the manner it was exposed to unauthorized third parties in the Data Breach.

45. By failing to protect Plaintiffs' and Class Members' Private Information, and by allowing the Data Breach to occur, 23andMe broke these promises to Plaintiffs and Class Members.

E. 23andMe Acquires, Collects and Stores Its Customers' Private Information.

46. 23andMe acquires, collects, and stores a massive amount of its customers' Private Information.

47. As a condition of engaging in their services, 23andMe requires that these customers entrust them with highly confidential Private Information.

48. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, 23andMe assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

49. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, and, as current and former customers, they relied on 23andMe to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

F. The Value of Private Information and the Effects of Unauthorized Disclosure.

50. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiffs and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

51. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[14] Indeed, a robust "cyber black market" exists in

[14] Federal Trade Commission, Warning Signs of Identity Theft, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Oct. 12, 2023).

which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

52. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363 according to the Infosec Institute.[15]

53. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

54. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[16]

55. Similarly, the FBI Cyber Division, in an April 8, 2014, Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

56. The ramifications of 23andMe's failure to keep its customers' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

---

[15] Center for Internet Security, Data Breaches: In the Healthcare Sector, available at: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last accessed Oct. 12, 2023).

[16] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed Oct. 12, 2023)

57. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

58. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.

59. Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage. Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

60. As a provider of DNA testing services, 23andMe knew, or should have known, the importance of safeguarding its customers' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on 23andMe's customers as a result of a breach. 23andMe failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

61. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to

identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[17] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[18] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information of Plaintiffs and Class Members that were misused.

62. Further, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

63. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts, particularly when they have easily-decrypted passwords and security questions.

64. The Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

G. 23andMe's Conduct Violates HIPAA.

65. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[19]

66. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the

[17] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report 35-38 (Dec. 2010), available at: https://www.ftc.gov/sites/default/files/documents/reports/federal-tradecommission-bureau-consumer-protection-preliminary-ftc-staff-report-protectingconsumer/101201privacyreport.pdf (as of April 18, 2021).

[18] *See id*. (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

[19] HIPAA Journal, What is Considered Protected Health Information Under HIPAA?, available at: https://www.hipaajournal.com/what-is-considered-protected-health-informationunder-hipaa/ (last accessed Oct. 12, 2023).

Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

67. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[20]

68. Based on information and belief, Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. 23andMe's security failures include, but are not limited to, the following:

a) Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b) Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

c) Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

d) Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

e) Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

[20] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Oct. 11, 2023).

f) Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

g) Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

h) Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, et seq. ;

i) Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

H. 23andMe Failed to Comply with FTC Guidelines.

69. 23andMe was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

70. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices.

According to the FTC, the need for data security should be factored into all business decision-making.[21]

71. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business,* which established cybersecurity guidelines for businesses.[22] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

72. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

73. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

74. 23andMe failed to properly implement basic data security practices. 23andMe's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[21] Federal Trade Commission, Start With Security: A Guide for Business, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Oct. 12, 2023).

[22] Federal Trade Commission, Protecting Personal Information: A Guide for Business, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf (last accessed Oct. 12, 2023).

75. 23andMe was at all times fully aware of its obligation to protect the Private Information of customers because of its position as a trusted healthcare provider.[23] 23andMe was also aware of the significant repercussions that would result from its failure to do so.

I. 23andMe Failed to Comply with Healthcare Industry Standards.

76. HHS's Office for Civil Rights notes:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[24]

77. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

78. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because the of value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[25] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

79. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, 23andMe chose to ignore them. These best practices were known, or should have been known by 23andMe, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

---

[23] https://blog.23andme.com/articles/data-privacy-certifications.

[24] HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last accessed Oct. 12, 2023).

[25] See e.g., INFOSEC, 10 Best Practices For Healthcare Security, available at: https://resources.infosecinstitute.com/topics/healthcare-information-security/10-best-practices-healthcare-security/ (last accessed Oct. 12, 2023).

J. Plaintiffs and Class Members Suffered Damages.

80. The ramifications of 23andMe's failure to keep customers' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[26]

81. The state of California generally prohibits healthcare providers from disclosing a customer's confidential medical information without prior authorization. California's Confidentiality of Medical Information Act ("CMIA") (Cal. Civ. Code § 56.10(a)) states that "a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a customer of the provider of health care or enrollee or subscriber of a health care service plan without first obtaining an authorization except as provided in subdivision (b) or (c)." (See also Cal. Civ. Code §§ 1798.80, *et seq.*)

82. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiffs and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

83. Defendant further owed and breached its duty to Plaintiffs and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

84. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiffs' and Class

[26] 2014 LexisNexis True Cost of Fraud Study, available at: https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Oct. 12, 2023).

Members' Private Information as detailed above, and Plaintiffs are now at a heightened and increased risk of identity theft and fraud.

85. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

86. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

87. None of the Plaintiffs had their genetic information compromised through any other data breaches, to their knowledge.

88. Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in their agreements with 23andMe and they were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

89. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information has diminished in value.

90. The Private Information belonging to Plaintiffs and Class Members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

91. Plaintiffs' and Class Members' Private Information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing, particularly scam marketing which several Plaintiffs have experienced, without the

approval of Plaintiff and Class Members. Due to the Data Breach, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

92. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

93. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

94. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs' and Class Members' Private Information.

95. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

96. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[27]

[27] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, Victims of Identity Theft, 2012, December 2013, available at: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed Oct. 12, 2023).

97. 23andMe has not offered or provided victims any identity monitoring services or fraud insurance 23andMe's offer fails to address the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

98. Defendant does not appear to be taking any measures to assist Plaintiffs and Class Members other than telling them to reset their password if they do not have a strong password and enable multi-factor authentication on customer's 23andMe account. None of these recommendations, however, require Defendant to expend any effort to protect Plaintiffs' and Class Members' Private Information.

99. Defendants' failure to keep the PHI and PII of Plaintiffs and the Class secure has severe ramifications. Given the highly sensitive nature of the PHI and PII stolen in the Data Breach, email addresses, photos, first and last names, and dates of birth, DNA ancestry, hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and the Class now and into the indefinite future. As a result, Plaintiffs have suffered injury and faces an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

100. The PHI and PII exposed in the Data Breach is highly coveted and valuable on underground markets. Identity thieves can use the PHI and PII to: (a) commit insurance fraud; (b) obtain a fraudulent driver's license or ID card in the victim's name; (c) obtain fraudulent government benefits; (d) file a fraudulent tax return using the victim's information; (e) commit medical and healthcare-related fraud; (f) access financial and investment accounts and records; (g) engage in mortgage fraud; and/or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

101. Further, malicious actors often wait months or years to use the PHI and PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PHI

and PII, meaning individuals can be victims of several cybercrimes stemming from a single data breach.

102. Plaintiffs and Class Members have been damaged in several ways. All Plaintiffs and Class Members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiffs and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Certain Plaintiffs and Class members have also purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class members also suffered a loss of the inherent value of their Private Information.

103. PII stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen PII to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

104. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

a) The compromise, publication, theft and/or unauthorized use of their Private Information;

b) Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c) Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent

researching how to prevent, detect, contest and recover from identity theft and fraud;

d) The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fail to undertake appropriate measures to protect the Private Information in their possession;

e) Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and

f) Anxiety and distress resulting from fear of misuse of their genetic medical information.

105. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

CHOICE OF LAW

106. The State of California has a significant interest in regulating the conduct of businesses operating within its borders. California seeks to protect the rights and interests of all California residents and citizens of the United States against a company headquartered and doing business in California. California has a greater interest in the nationwide claims of Plaintiffs and members of the Nationwide Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

107. The corporate headquarters of 23andMe South San Francisco, California, is the "nerve center" of their business activities - the place where their officers direct, control, and coordinate the companies' activities, including their data security functions and policy, financial, and legal decisions.

108. 23andMe's response to the Data Breach at issue here, and corporate decisions surrounding such response, were made from and in California.

109. 23andMe's breaches of duty to Plaintiffs and Nationwide Class members emanated from California.

110. Application of California law to the Nationwide Class with respect to Plaintiffs' and Class Members' claims is neither arbitrary nor fundamentally unfair because California has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Nationwide Class.

111. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the nationwide common law claims of all Nationwide Class members. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, California's Unfair Competition Law and Confidentiality of Medical Information Act may be applied to non-resident plaintiffs as against 23andMe.

CLASS ALLEGATIONS

112. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

113. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

Nationwide Class: All individuals whose Private Information was compromised in the data breach first disclosed by 23andMe on or about October 6, 2023.

114. In the alternative to the Nationwide Class, Plaintiffs seek certification of the following state Sub-Classes:

Illinois Sub-Class: All persons residing in Illinois whose Private Information was compromised in the data breach first disclosed by 23andMe on or about October 6, 2023.

Wisconsin Sub-Class: All persons residing in Wisconsin whose Private Information was compromised in the data breach first disclosed by 23andMe on or about October 6, 2023.

115. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, current or former employees, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments,

agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

116. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

117. **Numerosity**, Fed R. Civ. P. 23(a)(1): The Nationwide Class, Nationwide Sub-Classes, and State Subclasses (the "Classes") are so numerous that joinder of all members is impracticable. Plaintiffs believe that thousands of customers' Private Information may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

118. **Commonality**, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a) When Defendant actually learned of the Data Breach and whether their response was adequate;

b) Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their Private Information;

c) Whether Defendant breached that duty;

d) Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class Members' Private Information;

e) Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class Members' PII/PHI;

f) Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class Members' PII/PHI secure and prevent loss or misuse of that Private Information;

g) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h) Whether Defendant caused Plaintiffs' and Class Members' damages;

i) Whether Defendant violated the law by failing to promptly notify Class Members that their Private Information had been compromised;

j) Whether Plaintiffs and the other Class Members are entitled to actual damages, identity and/or credit monitoring, and other monetary relief;

k) Whether Defendant violated the California Unfair Competition Law (Business & Professions Code § 17200, *et seq*); and

l) Whether Defendant violated the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq*.).

m) Whether Defendant disclosed the Plaintiffs and the Class members' genetic information to any third party;

n) Whether Defendant first obtained written authorization from Plaintiff and the Illinois Sub-Class before disclosing their genetic information;

o) Whether Defendant's conduct violates the Illinois Genetic Information Privacy Act, 410 ILCS 513, *et seq*. ("GIPA");

p) Whether Defendant's actions as described herein are unfair and oppressive and thus, in violation of the ILLINOIS CONSUMER FRAUD ACT, 815 ILCS § 505, *et seq*. ("ICFA");

q) Whether Defendant breached the confidentiality of Plaintiffs and the Wisconsin Sub-Class members' records in violation of Wis. Stat. 146.81, *et seq*.

r) Whether Defendant's actions as described herein constitute misrepresentations and thus, in violation of Wisconsin's Deceptive Trade Practices Act, Wis. Stat. §100.18 (the "WDTPA"); and

119. **Typicality**, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

120. **Adequacy**, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief

that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

121. **Superiority and Manageability**, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

122. **Policies Generally Applicable to the Class**: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

123. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that

experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

124. 23andMe based in South San Francisco, California, on information and belief, all managerial decisions emanate from there, the representations on 23andMe's website originate from there, 23andMe's misrepresentations originated from California, and therefore application of California law to the Nationwide Class is appropriate.

125. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

126. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

127. Unless a Class-wide injunction is issued, Plaintiffs and Class Members remain at risk that Defendant will continue to fail to properly secure the Private Information of Plaintiffs and Class Members resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Complaint.

128. Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

129. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a) Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b) Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c) Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e) Whether Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I

NEGLIGENCE

(On Behalf of Plaintiffs and the Classes)

130. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

131. As a condition of receiving services, Plaintiffs and Class Members were obligated to provide 23andMe with their Private Information.

132. Plaintiffs and Class Members entrusted their Private Information to 23andMe with the understanding that 23andMe would safeguard their information.

133. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

134. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing its security protocols to ensure that Private Information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on relevant cybersecurity measures.

135. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and Class Members, the critical importance of providing adequate security of that Private Information, the current cyber scams being perpetrated, and that they had inadequate employee training and education and IT security protocols in place to secure the Private Information of Plaintiffs and Class Members.

136. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein.

137. Plaintiffs and Class Members had no ability to protect their Private Information that was in Defendant's possession.

138. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

139. Defendant had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

140. Defendant has admitted that Plaintiffs' and Class Members' Private Information was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

141. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information while it was within Defendant's possession or control.

142. Defendant improperly and inadequately safeguarded Plaintiffs' and Class Members' Private Information in violation of standard industry rules, regulations, and practices at the time of the Data Breach.

143. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its Plaintiffs' and Class Members' Private Information.

144. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

145. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' Private Information would not have been compromised and/or subsequently misused by unauthorized third parties to engage in fraudulent activity further harming Plaintiffs and Class Members.

146. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Private Information and the harm suffered, or risk of imminent harm suffered, by Plaintiffs and the Class.

147. As a result of Defendant's negligence, unauthorized parties acquired Plaintiffs' Private Information and used that specific information to harm Plaintiffs and Class Members as described above. As a further result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer damages and injury including, but not limited to, (a) actual identity theft; (b) an increased risk of identity theft, fraud, and/or misuse of their Private Information; (c) the loss of the opportunity of how their Private Information is used; (d) the compromise, publication, and/or theft of their Private Information; (e) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (f) diminished value of the Private Information; (g) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (h) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (i) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

COUNT II

INVASION OF PRIVACY

(On Behalf of Plaintiffs and the Classes)

148. Plaintiffs restate and realleges all of the foregoing Paragraphs as if fully set forth herein.

149. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy with respect to their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

150. Defendant owed a duty to customers in their network, including Plaintiffs and Class Members, to keep their Private Information confidential.

151. The unauthorized release of Private Information, especially the type related to personal health information, is highly offensive to a reasonable person.

152. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their Private Information to Defendant as part of their use of Defendant's services, but privately, with the intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

153. The Data Breach constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

154. Defendant acted with a knowing state of mind when they permitted the Data Breach because they knew its information security practices were inadequate and would likely result in a data breach such as the one that harmed Plaintiffs and Class Members.

155. Acting with knowledge, Defendant had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

156. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' Private Information was disclosed to and used by third parties without authorization in the manner described above, causing Plaintiffs and Class Members to suffer damages.

157. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons.

158. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

COUNT III

BREACH OF CONTRACT

(On Behalf of Plaintiffs and the Classes)

159. Plaintiffs restate and realleges all of the foregoing Paragraphs as if fully set forth.

160. Plaintiffs and other Class Members entered into valid and enforceable express contracts with Defendant under which Plaintiffs and other Class Members agreed to provide their Private Information (including their genetic information) to Defendant, and Defendant agreed to provide genetic testing for monetary compensation and, impliedly if not explicitly, agreed to protect Plaintiffs' and other Class Members' Private Information.

161. To the extent Defendant's obligation to protect Plaintiffs' and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and other Class Members' Private Information, including in accordance with HIPAA regulations; federal, state and local laws; and industry standards. No Plaintiff would have entered into these contracts with Defendant without understanding that Plaintiffs' and other Class Members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

162. Both the provision of DNA testing and the protection of Plaintiffs' and other Class Members' Private Information were material aspects of Plaintiffs' and other Class Members' contracts with Defendant.

163. Defendant's promises and representations described above relating to HIPAA, CMIA, and industry practices, and about Defendant's purported concern about their customers' privacy rights became terms of the contracts between Defendant and their customers, including Plaintiffs and other Class Members. Defendant breached these promises by failing to comply with HIPAA, CMIA, and reasonable industry practices.

164. Plaintiffs and Class Members read, reviewed, and/or relied on statements made by or provided by 23andMe and/or otherwise understood that 23andMe would protect its customers' Private Information if that information were provided to 23andMe.

165. Plaintiffs and Class Members fully performed their obligations under the contract with Defendant; however, Defendant did not.

166. As a result of Defendant's breach of these terms, Plaintiffs and other Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, and Plaintiffs and other Class Members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take months if not years to manifest, discover, and detect.

167. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT IV

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs and the Classes, in the Alternative to Count III)

168. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

169. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of their use of Defendant's services. By providing their Private Information, and upon Defendant's acceptance of such information, Plaintiffs and all Class Members, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contracts concerning genetic testing or other services to be provided by Defendant to Plaintiffs.

170. These implied-in-fact contracts obligated Defendant to take reasonable steps to secure and safeguard Plaintiffs' and other Class Members' Private Information. The terms of these implied contracts are further described in the federal laws, state laws, and industry standards

alleged above, and Defendant expressly assented to these terms in their Notice of Privacy Practices and other public statement described above.

171. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services, along with Defendant's promise to protect their Private Information from unauthorized disclosure.

172. In their written privacy policies, 23andMe expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

173. 23andMe promised to comply with HIPAA standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

174. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide Private Information was Defendant's obligation to (a) use such Private Information for business purposes only; (b) take reasonable steps to safeguard that Private Information; (c) prevent unauthorized disclosures of the Private Information; (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses; and (f) retain the Private Information only under conditions that kept such information secure and confidential.

175. Without such implied contracts, Plaintiffs and Class Members would not have provided their Private Information to Defendant.

176. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

177. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to conduct the following: 1) reasonably safeguard and protect Plaintiffs' and Class Members' Private Information, which was compromised as a result of the Data Breach; 2) comply with their promise to abide by HIPAA; 3) ensure the confidentiality and integrity of electronic protected health information that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R 164.306(a)(1); 4) implement technical policies and procedures for

electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R 164.312(a)(1); 5) implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R 164.308(a)(1); 6) identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R 164.308(a)(6)(ii); and 7) protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R 164.306(a)(2).

178. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and other Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, and Plaintiffs and other Class Members have been put at an increased risk of identity theft, fraud, and/or misuse of their Private Information, which may take months if not years to manifest, discover, and detect.

COUNT V

UNJUST ENRICHMENT

(On Behalf of Plaintiffs and the Classes)

179. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

180. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

181. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

182. The amounts Plaintiffs and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

183. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

184. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

185. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

186. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to Defendant's services.

187. Plaintiffs and Class Members have no adequate remedy at law.

188. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) an increased risk of identity theft, fraud, and/or misuse of their Private Information; (c) the loss of the opportunity of how their Private Information is used; (d) the compromise, publication, and/or theft of their Private Information; (e) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (f) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (g) the continued risk to their Private Information, which remains in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (h) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

189. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

190. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT VI

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, *ET SEQ.* - UNLAWFUL, FRAUDULENT, AND UNFAIR BUSINESS PRACTICES

(On Behalf of Plaintiffs and the Classes)

191. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

192. The California Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200 *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

193. By reason of Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs and Class members' Private Information, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

194. Defendant has violated Cal. Bus. and Prof. Code § 17200, et seq., by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or

misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Nationwide Class.

195. Defendant's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the Private Information of Plaintiffs and Class Members has been compromised for unauthorized parties to see, use, and otherwise exploit.

196. Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information also constitute "unfair" business acts and practices within the meaning of Business & Professions Code sections 17200 *et seq*., in that Defendant's conduct was substantially injurious to Plaintiffs and Class Members, offensive to public policy, immoral, unethical, oppressive and unscrupulous, and the gravity of Defendant's conduct outweighs any alleged benefits attributable to such conduct.

197. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' Private Information with knowledge that the information would not be adequately protected; by violating the California Confidentiality Of Medical Information Act, Cal. Civ. Code § 56, *et seq*. ; by violating the other statutes described above; and by storing Plaintiffs' and Class Members' Private Information in an unsecure electronic environment in violation of HIPAA and California's data breach statute, Cal. Civ. Code § 1798.81.5, which require Defendant to take reasonable methods of safeguarding the Private Information of Plaintiffs and the Class Members.

198. Defendant's practices were also unlawful and in violation of Civil Code sections 1798 et seq. and Defendant's own privacy policy because Defendant failed to take reasonable measures to protect Plaintiffs' and Class Members' Private Information and failed to take remedial measures such as notifying its users when it first discovered that their Private Information may have been compromised.

199. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82 and Cal. Health & Safety Code §1280.15(b)(2).

200. Defendant's business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the Private Information, they provided to Defendant will remain private and secure, when in fact it has not been maintained in a private and secure manner, and that Defendant would take proper measures to investigate and remediate a data breach, when Defendant did not do so.

201. Plaintiffs and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendant's above-described wrongful actions, inaction, and omissions including, inter alia, the unauthorized release and disclosure of their Private Information and lack of notice.

202. But for Defendant's misrepresentations and omissions, Plaintiffs and Class Members would not have provided their Private Information to Defendant or would have insisted that their Private Information be more securely protected.

203. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiffs and Class Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described herein.

204. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' Private Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

205. Plaintiffs, on behalf of the Class, seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and Class Members of money or property that Defendant may have acquired by means of Defendant's unlawful, and unfair

business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VII

VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE § 56, *ET SEQ.*

(On Behalf of Plaintiffs and the Classes)

206. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

207. At all relevant times, Defendant was a health care provider because it had the "purpose of maintaining medical information to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual."

208. Defendant is a provider of healthcare within the meaning of Civil Code § 56.06(a) and maintains medical information as defined by Civil Code § 56.05.

209. Plaintiffs and Class Members are customers of Defendant, as defined in Civil Code § 56.05(k).

210. Plaintiffs and Class Members provided their personal medical information to Defendant.

211. At all relevant times, Defendant collected, stored, managed, and transmitted Plaintiff's and Class Members' personal medical information.

212. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a customer of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization."

213. As a result of the Data Breach, Defendant has misused, disclosed, and/or allowed third parties to access and view Plaintiffs' and Class Members' personal medical information without their written authorization compliant with the provisions of Civil Code §§ 56, *et seq*.

214. The hacker or hackers who committed the Data Breach obtained Plaintiffs' and Class Members' personal medical information, viewed it, and now have it available to them to sell to others bad actors or otherwise misuse.

215. As a further result of the Data Breach, the confidential nature of the plaintiff's medical information was breached as a result of Defendant's negligence. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties to access and view Plaintiff's and Class Members' Private Information, which was viewed and used when the unauthorized parties engaged in the above-described fraudulent activity.

216. Defendant's misuse and/or disclosure of medical information regarding Plaintiffs and Class Members constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

217. Additionally, because Defendant collects and analyzes genetic information about Plaintiffs and that information appears to have been disclosed or stolen in the Data Breach due to Defendant's negligence, Defendant is liable for the statutory penalties under Civil Code §§ 56.17(b) and 56.17(d).

218. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care, Plaintiffs' and Class Members' personal medical information was disclosed without written authorization.

219. By disclosing Plaintiffs' and Class Members' Private Information without their written authorization, Defendant violated California Civil Code § 56, *et seq*., and their legal duty to protect the confidentiality of such information.

220. Defendant also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

221. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach,

Plaintiffs' and Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiffs' and Class Members' written authorization.

222. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violation of the CMIA, Plaintiffs and Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and Class Member, (iii) punitive damages of up to $3,000 per Plaintiff and Class Member, and (iv) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

COUNT VIII

VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT CAL. CIV. CODE § 17598, *ET SEQ.*

(On Behalf of Plaintiffs and the Classes)

223. Plaintiffs incorporate by reference the allegations contained in each and every paragraph of this Complaint.

224. The California Consumer Privacy Act ("CCPA"), portions of which were operative beginning January 1, 2020, was enacted by the California Legislature "to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80)." Cal. Civ. Code § 1798.100. The CCPA applies to "the collection and sale of all personal information collected by a business from consumers." *Id*.

225. "Businesses," defined to include a "corporation" that "collects consumers' personal information" that "does business in the State of California" and has annual gross revenues in excess of $25 million, are required to comply with the CCPA. Cal. Civ. Code §1798.140(c). Defendant is a "business" under the CCPA.

226. The CCPA protects "consumers." "Consumer" is defined as "a natural person who is a California resident[.]" Cal. Civ. Code § 1798.140(g). Plaintiffs and members of the California Subclass are "consumers" within the meaning of the CCPA.

227. The protections of the CCPA extend to "personal information" of consumers. "Personal information" is defined by the CCPA to include "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(o)(1). "Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (A) Identifiers such as... driver's license number, ..." Cal. Civ. Code § 1798.140(o)(1)(A). The PII of Plaintiffs and members of the California Subclass that was compromised in Defendant's data breach included "personal information" within the meaning of the CCPA.

228. The CCPA provides consumers with the right to institute a civil action where the consumers' "nonencrypted and nonredacted personal information" was the subject of "an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Cal. Civ. Code § 798.150(a)(1).

229. Plaintiffs and California Subclass members provided to Defendant their nonencrypted and nonredacted personal information as defined in § 1798.81.5 in the form of their PII.

230. Defendant, as a "business" covered by the CCPA, owed a duty to Plaintiffs and members of the California Subclass to implement and maintain reasonable security procedures and practices to protect the PII of Plaintiffs and members of the California Subclass.

231. Defendant breached this duty. The fact that Plaintiffs' and the California Subclass's PII was accessed without authorization establishes that Defendant did not take adequate data security measures to store and protect its customers' PII. Defendant failed to take adequate security measures to protect Plaintiffs' and the California Subclass members' PII.

232. As a direct and proximate result of Defendant's acts and omissions, Plaintiffs and the members of the California Subclass were subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty.

233. On behalf of the California Subclass, Plaintiffs seeks injunctive relief in the form of an order (a) enjoining Defendant from continuing to violate the CCPA; and (b) requiring Defendant to employ adequate security practices consistent with law and industry standards to protect class members' PII.

234. Plaintiffs and California Subclass members are at high risk of suffering, or have already suffered, injuries that cannot be remedied monetarily, such as reductions to their credit scores and identity theft. As such, the remedies at law available to Plaintiffs and California Subclass members are wholly inadequate by themselves.

235. The full extent of the existing and potential harm caused by Defendant's failure to protect its customers' PII cannot be remedied by monetary damages alone because monetary compensation does nothing to prevent the reoccurrence of another data breach in the future.

236. Plaintiffs presently seek only injunctive relief and any other relief the court deems proper pursuant to this section, such as attorneys' fees.

COUNT IX

INJUNCTIVE/DECLARATORY RELIEF

(On Behalf of Plaintiffs and the Nationwide Class)

237. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

238. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

239. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the Private Information they collected from Plaintiffs and Class Members.

240. Defendant owes a duty of care to Plaintiffs and Class Members requiring them to adequately secure Private Information.

241. Defendant still possesses Private Information regarding Plaintiffs and Class Members.

242. Since the Data Breach, Defendant have announced few if any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

243. Defendant have not satisfied their contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattack.

244. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that lead to such exposure.

245. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties. Plaintiffs therefore seek a declaration (1) that Defendant's existing security measures do not comply with their contractual obligation and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures.

COUNT X

Illinois Genetic Information Privacy Act, 410 ILCS 513/1, *et seq*.

(On Behalf of Plaintiffs Berman, Jones, Leifer and the Illinois Sub-Class)

246. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

247. Defendant is a corporation and, therefore, a "person" under 410 ILCS 513/10.

248. GIPA provides a private right of action for violations. 410 ILCS 513/40(a).

249. Plaintiffs and the Illinois Sub-Class obtained "genetic test[s]" and received the results of such tests from Defendant.

250. Defendant's disclosure of sensitive genetic information violates GIPA, which makes it unlawful for companies that collect genetic information to disclose such information without first obtaining written authorization.

251. Plaintiffs and the Illinois Sub-Class also provided accompanying personal identifying information, including their full names, email address, and/or home addresses (including age, birthday, and gender in some instances) to Defendant.

252. Defendant disclosed and/or released Plaintiffs' and the Class members' genetic tests and/or information derived from their genetic tests (genetic information), along with their accompanying personal identifying information

253. Defendant did not receive any written authorization from Plaintiffs or the members of the Illinois Sub-Class to disclose and/or release their genetic test results and information derived therefrom, including their personal identifying information, as mandated by 410 ILCS 513/15(a) and 410 ILCS 513/30(a)(2).

254. The information obtained from Plaintiffs and the Class by Defendant is the type of information protected by GIPA. 410 ILCS 513/10.

255. Defendant's negligent practices led to disclosing its customers' genetic information to third parties without first obtaining consent.

256. Defendant's negligence poses serious and irreversible privacy risks to its customers.

257. Plaintiffs and the Illinois Sub-Class members have been aggrieved by Defendant's violations of their statutorily protected rights to privacy in their genetic information as set forth in GIPA when Defendant disclosed and/or released their statutorily protected genetic information without their consent to Blackstone and/or others.

258. GIPA provides for statutory damages of $15,000 for each willful and/or reckless violation of GIPA or actual damages – whichever is greater – and, alternatively, damages of $2,500 for each negligent violation of GIPA or actual damages – whichever is greater; GIPA also

provides for reasonable attorney's fees and costs, including expert witness fees and other litigation expenses. 410 ILCS 513/40(a)(1)-(3).

COUNT XI

Illinois Consumer Fraud Act, 815 ILCS § 505, *et seq*.

(On Behalf of Plaintiffs Berman, Jones, Leifer and the Illinois Sub-Class)

259. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

260. The ICFA is a "regulatory and remedial statute intended to protect consumers, borrowers, and business persons against fraud, unfair methods of competition, and other unfair and deceptive business practices." *Robinson v. Toyota Motor Credit Corp*., 201 Ill.2d 403, 41617 (2002); *Hill v. PS Illinois Trust*, 368 Ill.App.3d 310, 319 (1st Dist. 2006). It is to be liberally construed to effectuate its purpose. *Robinson*, 201 Ill.2d at 417.

261. Recovery under ICFA may be had for unfair as well as deceptive conduct. *Robinson*, 201 Ill.2d at 417. In determining whether conduct is unfair under the Act, courts consider (1) whether the practice offends public policy; (2) whether it is oppressive, immoral, unethical, or unscrupulous; and (3) whether it causes consumers substantial injury. *Boyd v. U.S. Bank, N.A*., 787 F. Supp. 2d 747, 751 (N.D. Ill. 2011); *Dubey v. Public Storage, Inc.*, 395 Ill.App.3d 342, 354 (1st Dist. 2009). A practice can be unfair without meeting all three criteria. *Id*.

262. A practice offends public policy "if it violates a standard of conduct contained in an existing statute or common law doctrine that typically applies to such a situation." *Boyd*, 787 F. Supp. 2d at 752; *Beatty v. Accident Fund General Insurance Co*., 2018 WL 3219936, at *12 (S.D. Ill. 2018). In other words, a plaintiff may base an ICFA claim on violations of other statutes or regulations, which alone do not allow for private enforcement. *Boyd*, 787 F. Supp. 2d at 752. Accordingly, "[v]iolations of agency directives … can be a hallmark of unfairness under ICFA." *Id*. at 753.

263. Here, 23andMe's conduct is unfair under ICFA. First, 23andMe violated numerous regulations regarding HIPAA guidelines for safeguarding PHI and PII. In allowing the Data

Breach to occur, 23andMe failed to: (a) ensure the confidentiality, integrity, and availability of all electronic protected health information the entity creates, receives, maintains, or transmits (45 C.F.R. § 164.306(a)(1)); (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information (45 C.F.R. § 164.306(a)(2)); (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required (45 C.F.R. § 164.306(a)(3)); (d) implement policies and procedures to prevent, detect, contain, and correct security violations (45 C.F.R. § 164.308(1)); (e) implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights (45 C.F.R. § 164.312(a)(1)); (f) have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (45 C.F.R. § 164.530(c)(1)); and (g) mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information (45 C.F.R. § 164.530(f)). Accordingly, 23andMe's inability to safeguard Plaintiff's and Class Members' Personal Information offends public policy.

264. Second, 23andMe's conduct against Plaintiff and the Class is oppressive in that even a request to delete data does not securely delete all data.[28] Plaintiff and the Class were assured by 23andMe that their Personal Information would be secured.

265. And third, 23andMe's failure to safeguard Plaintiff's and Class Members' Personal Information and leaving it exposed to cybercriminals and other unauthorized actors constitutes a substantial injury in that Plaintiff and the Class will not only have to spend the remainder of their lives at greater risk for identity theft and fraud (having to constantly monitor for the same), but also live with the knowledge that their most intimate medical details are subject to public view.

266. Finally, 23andMe violated FTC guidelines by failing to: promptly encrypt information stored on computer networks; understand vulnerabilities of its network; implement policies to correct security problems; use an intrusion detection system to expose a breach as soon

[28] https://www.23andme.com/legal/privacy/#other-things-to-know

as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. These failures constitute unfair acts or practices, subjecting them to an ICFA claim. 15 U.S.C. § 45.

267. In sum, 23andMe's numerous failures in safeguarding Plaintiff's and Class Members' Personal Information violates ICFA.

268. Pursuant to Section 5 of the FTC Act, failure to protect Personal Information can constitute an unfair act or practice.

269. The state of Illinois has also addressed the protection of Personal Information by enacting the Personal Information Protection Act ("PIPA"), 815 ILCS 530/1 *et seq*.

270. PIPA requires "...implement[ation] and maintain[enance of] reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure" of PHI by data collectors. 815 ILCS 530/45.

271. Failure to comply with PIPA constitutes an unlawful practice under ICFA. 815 ILCS § 530/20.

272. As a result, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (a) the compromise, publication, theft, and /or unauthorized use of their Personal Information: (b) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft and fraud; (c) lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; (d) the continued risk to the publication of their Personal Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect Personal Information in their possession; and (e) current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and the Classes.

273. 23andMe's failure to safeguard Plaintiff's and Class Members' Personal Information in violation of HIPAA and FTC Act, PIPA and common violations were the direct and proximate cause of damages incurred by Plaintiff and the Class.

274. Accordingly, Plaintiff, on behalf of herself and the other members of the Classes, seeks compensatory damages for the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs as provided by 818 ILCS § 505/10(a) and, in the event that 23andMe's violations are found to be willful, punitive damages.[29]

275. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

COUNT XII

Breach of Confidentiality of Health Records, Wis. Stat. 146.81, et seq.

(On Behalf of Plaintiff Loftus and the Wisconsin Sub-Class)

276. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

277. Wisconsin law regarding Confidentiality of Patient Health Care Records, Wis. Stat. §§ 146.81, et seq., states that:

> "All patient health care records shall remain confidential. Patient health care records may be released only to the persons designated in this section or to otherpersons with the informed consent of the patient or of a person authorized by thepatient." Wis. Stat. § 146.82(1).

278. The stolen PHI belonging to Plaintiffs and the Class Members are "Health care records" under Wis. Stat. § 146.81(4).[30]

279. Defendant violated Wis. Stat. §§ 146.81, et seq. when it compromised, allowed access to, released, and disclosed patient health care records and PHI to third parties without the informed consent or authorization of Plaintiffs and the Class Members. Defendant did not and does not have express or implied consent to disclose, allow access to, or release Plaintiffs' and the

[29] Pursuant to 815 ILCS 505/10a(d), Plaintiffs are serving a copy of this Complaint on the Illinois Attorney General.

[30] "Patient health care records' means all records related to the health of a patient prepared by or under the supervision of a health care provider; . . ." Wis. Stat. § 146.81(4).

Class Members' PHI. To the contrary, Defendant expressly undertook a duty and obligation to Plaintiffs and Class Members when it told them their PHI would be private and secure.

280. Defendant did not disclose to or warn Plaintiffs and Class Members that their PHI could be compromised, stolen, released, or disclosed to third parties without their consent because of Defendant's computer systems and software being outdated, easy to hack, inadequate, and insecure. Plaintiffs and Class Members did not know or expect, or have any reason to know or suspect, that Defendant's computer systems and software were so outdated, easy to hack, inadequate, and insecure that it would expose their PHI to unauthorized disclosure. In fact, they were told to the contrary in written statements and representations given to Plaintiffs and Class Members, and on 23andMe's website, namely that:

- We exceed industry data protection standards and have achieved 3 different ISO certifications to demonstrate the strength of our security program.
- We encrypt all sensitive information and conduct regular assessments to identify security vulnerabilities and threats.
- We will not release any individual-level personal information to law enforcement unless we are required to do so by court order, subpoena, search warrant or other requests that we determine are legally valid.[31]

281. Wis. Stat. § 146.84(1)(b) states:

> Any person, including the state or any political subdivision of the state, who violates Wis. Stat. s. 146.82 or 146.83 in a manner that is knowing and willful shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $25,000 and costs and reasonable actual attorney fees."

282. Wis. Stat. § 146.84(1)(bm) states:

> "Any person, including the state or any political subdivision of the state, who negligently violates Wis. Stat. s. 146.82 or 146.83 shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $1,000 and costs and reasonable actual attorney fees." Wis. Stat. § 146.84(1)(bm).

283. Wis. Stat. § 146.84(1)(c) states:

> "An individual may bring an action to enjoin any violation of s. 146.82 or 146.83 or to compel compliance with s. 146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection."

[31] https://www.23andme.com/privacy/

284. Actual damages are not a prerequisite to liability for statutory or exemplary damages under Wis. Stat. § 146.81. A simple comparison of other Wisconsin statues (e.g., Wis. Stat. § 134.97(3)(a) and (b), "Civil Liability; Disposal And Use" of records containing personal information), makes clear that the Wisconsin Legislature did not include an actual damages requirement in Wis. Stat. § 146.84 when it explicitly did so in other privacy statutes. See Wis. Stat. § 134.97(3)(a) and (b).[32]

285. Similarly, the Wisconsin Legislature made it clear that the exemplary damages referred to in Wis. Stat. § 146.81 are not the same as punitive damages. Here, the plain language of another Wisconsin statue (Wis. Stat. § 895.043(2), "Scope" of punitive damages), specifically and unequivocally excludes an award of "exemplary damages" under Wis. Stat. §§ 146.84(1)(b) and (bm) from the scope of "punitive damages" available under Section 895.043.19 In short, exemplary damages under Wis. Stat. § 146.84(1)(b) and (bm) are not the same as either actual damages, or punitive damages; they are statutory damages available to persons who have been injured as a result of a negligent data breach like the one at issue here.

286. Black's Online Law Dictionary, Online 2nd Ed. defines "injury" as:

> "Any wrong or damage done to another, either In his person, rights, reputation, or property. Parker v. Griswold, 17 Conn. 298, 42 Am. Dec. 739; Woodruff v. Mining Co., 18 Fed. 781; Hitch v. Edgecombe County, 132 N. C. 573, 44 S. E. 30; Macauley v. Tierney, 19 R. I. 255, 33 Atl. 1, 37 L. R. A. 455, 61 Am. St. Rep. 770. In the civil law. A delict committed in contempt or outrage of any one, whereby his body, his dignity, or his reputation is maliciously injured. Voet, Com. ad Pand. 47, t. 10, no. 1."

287. Plaintiffs and the Wisconsin Sub-Class request that the Court issue declaratory relief declaring 23andMe's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of PHI data between 23andMe and third parties unlawful. Plaintiffs and the Wisconsin Sub-Class further request the Court enter an injunction requiring 23andMe to cease the unlawful practices described

[32] "A financial institution, medical business or tax preparation business is liable to a person whose personal information is disposed of in violation of sub. (2) for the amount of damages *resulting from the violation*." Wis. Stat. § 134.97(3)(a) (emphasis added).

herein, and enjoining Defendant from disclosing or using PHI without first adequately securing or encrypting it.

288. Plaintiffs and the Wisconsin Sub-Class request the Court order Defendant to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing PHI of Plaintiffs and the Wisconsin Sub-Class in their possession or the possession of third parties and provide it to Plaintiffs and the Wisconsin Sub-Class.

289. Plaintiffs and the Class Members request that the Court enter an injunction ordering that Defendant:

(a) engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct test, and audit Defendant's safeguards and procedures on a periodic basis;
(b) audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;
(c) conduct regular checks and tests on its safeguards and procedures;
(d) periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;
(e) meaningfully educate its former and current patients about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps Defendant is taking to update its security technology to adequately secure and safeguard patient PHI; and
(f) identify to each Class Member in writing with reasonable specificity the PHI and personal information of each such Class Member that was stolen in the Data Breach, including without limitation as required under Wis. Stat. § 134.98(3)(c).

290. Plaintiffs and the Class Members request the Court enter an order pursuant to Wis. Stat. § 146.84(1)(bm) awarding minimum statutory exemplary damages of $1,000 to Plaintiffs and the Wisconsin Sub-Class whose PHI was compromised and stolen, as well as attorneys' fees and costs.

COUNT XIII

Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§100.18, *et seq*.

(On Behalf of Plaintiff Loftus and the Wisconsin Sub-Class)

291. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

292. 23andMe's conduct violates WDTPA, which provides that no "firm, corporation or association ... with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading." Plaintiffs and the Class Members "suffer[ed] pecuniary loss because of a violation" of the WDTPA. Wis. Stat. § 100.18(11)(b)(2).

293. 23andMe's deliberately engaged in deceptive and unlawful practices when it issued public announcements, statements, and representations, including in press releases, on Defendant's website, and in the Notice Letter, in violation of Wisconsin law by failing to include in its representations to Plaintiffs and the Wisconsin Sub-Class Members and the public the scope of the Data Breach, when 23andMe knew the scope because the breached records were already available on the dark web.

294. 23andMe deliberately engaged in deceptive and unlawful practices when it issued announcements, statements, and representations, including in press releases, on 23andMe's website, and in the direct notice to Plaintiffs and the Wisconsin Sub-Class, in violation of Wisconsin law by representing to Plaintiffs, the Wisconsin Sub-Class, and the public that 23andMe did not know what specific PHI was stolen, when in fact, they did have said information and knowledge. The purpose of 23andMe's misrepresentations was to minimize the harm and injury-in-fact Plaintiffs and the Wisconsin Sub-Class are facing caused by the Data Breach, and therefore increase the sales and use of 23andMe's services.

295. Plaintiffs and the Wisconsin Sub-Class relied upon 23andMe's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all members of the Classes, request judgment against the Defendant and that the Court grant the following relief:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Classes requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein;

B. Injunctive relief requiring Defendant to take appropriate measures to strengthen their data security systems that maintain personally identifying and other information to comply with the applicable state laws according to proof;

C. An order requiring Defendant to pay all costs associated with class notice and administration of class-wide relief;

D. An award to Plaintiff and all members of the Classes of compensatory, consequential, incidental, nominal, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

E. An award of nominal damages of $1,000 per Plaintiff and Class Member to Plaintiff and all members of the Classes under California Civil Code § 56.35;

F. An award of punitive damages of up to $3,000 per Plaintiff and Class Member under California Civil Code § 56.35;

G. An award of credit monitoring and identity theft protection services to Plaintiff and all members of the Classes

H. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

I. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

J. An order requiring Defendant to pay pre-judgment and post-judgment interest, as provided by law or equity;

K. An award to Plaintiff and all members of the Illinois Sub-Class of either $15,000 or $2,500 per violation of GIPA plus attorney's fees and costs, including expert witness

fees and other litigation expenses

L. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PHI;

M. Order disgorgement of Defendant' unjustly acquired revenue, profits, and other benefits resulting from their unlawful conduct for the benefit of Plaintiffs and the Wisconsin Sub-Class in an equitable and efficient manner determined by the Court;

N. Order the imposition of a constructive trust upon Defendant such that its enrichment, benefit, and ill-gotten gains may be allocated and distributed equitably by the Court to and for the benefit of Plaintiffs and the Wisconsin Sub-Class; and

O. Such other and further relief as this Court may deem just and proper.

Dated: October 19, 2023

Respectfully submitted,

LOFTUS & EISENBERG, LTD.

By: /s/*Ross M. Good*
Ross M. Good
Attorneys for Plaintiffs

Ross M. Good, Esq.
LOFTUS & EISENBERG, LTD.
161 N. Clark, Suite 1600
Chicago, Illinois 60601
T: (312) 889-6625
ross@loftusandeisenberg.com
Pro Hac Vice

William Aron, Esq.
ARON LAW FIRM
15 W Carrillo St, Suite 217
Santa Barbara, CA 93101
T: (805) 618-1768
bill@aronlawfirm.com